AF/ IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kelly E. Dillard et al.

Title: COPY PROTECTION FOR DATABASE UPDATES TRANSMITTED VIA THE INTERNET

Docket No.: 462-96-004 (256.180US1) Serial No.: 08/861,989
Filed: May 22, 1997 Due Date: August 10, 2004
Examiner: Jeffrey D. Carlson Group Art Unit: 3622

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X A return postcard.
X Appellant's Brief On Appeal (13 Pages) (in triplicate).

If not provided for in a separate paper filed herewith, Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: Monique M. Perdok Shonka
Atty: Monique M Perdok Shonka
Reg. No. 42,989

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief--Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 10th day of August, 2004.

Dawn M. Bole
Name

Dawn M. Bole
Signature

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Kelly E. Dillard et al.	)	Examiner: Jeffrey D. Carlson
	)	
Serial No.: 08/861,989	)	Group Art Unit: 3622
	)	
Filed: May 22, 1997	)	Docket: 462-96-004 (256.180US1)
	)	
For: COPY PROTECTION FOR DATABASE UPDATES TRANSMITTED VIA THE INTERNET	)	

APPELLANTS' BRIEF ON APPEAL

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on June 10, 2004, from the Final Rejection of claims 25-30 of the above-identified application, as set forth in the Final Office Action mailed on December 10, 2003.

This Appeal Brief is filed in triplicate. The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of $330.00 which represents the requisite fee set forth in 37 C.F.R. § 117. The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims.

APPELLANTS' BRIEF ON APPEAL

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, HONEYWELL INTERNATIONAL INC..

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 25-30 are pending in the application and have all been finally rejected. The rejected claims 25-30 are the subject of the present appeal.

4. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action mailed to the Appellants on December 10, 2003.

5. SUMMARY OF THE INVENTION

The present invention is a system for protecting the unauthorized use of software transmitted over a communication link. Previously, updates of topographical and navigational databases have been mailed to customers after an order is placed with a software supplier, as discussed in the background. Such an order may take days or weeks to fill depending on the

location of the customer. Once the updated database is in the control of the customer, it may be easily used in multiple devices even if additional updates have not been purchased.

By transferring the updated data over a communication link rather than mailing a storage device such as a diskette, the database may be updated almost instantaneously rather than in a few days time. This service becomes increasingly valuable as the information contained in the database changes more rapidly. For example, a database containing road information, such as closings or delays due to construction, may be valuable only if received quickly.

The information transferred is protected by an encryption algorithm that prevents devices other than the intended recipient from accessing the information. Page 8, lines 29-35. For example, a global positioning system (GPS) unit stores a software key. The key is unique across the multitude of such devices, so that each device may be individually identified by a software supplier. The GPS unit requests updated navigation data, such as road maps. The request is sent to the software supplier along with the key and payment information such as a credit card to be billed. The transfer is authorized, and the requested information is encoded based on the software key. The encrypted information is sent to the GPS unit and updates the existing database. No other GPS unit would be able to use the data, because other units do not possess the software key.

6. ISSUES PRESENTED FOR REVIEW

Whether claims 25-30 are patentable under 35 USC § 103(a) over Behr et al. (U.S. Patent No. 6,107,944) in view of Hornbuckle (WO 90/13865) and Ahrens et al. (U.S. Patent No. 5,951,620).

7. GROUPING OF CLAIMS

Claims 25-30 are grouped together for the purposes of this appeal.

8. ARGUMENT

1) The Applicable Law

The Examiner has the burden under 35 U.S.C. 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). As part of establishing a *prima facie* case of obviousness, the Examiner must show that some objective teaching in the prior art or some knowledge generally available to one of ordinary skill in the art would lead an individual to combine the relevant teaching of the references. *Id.*

The court in *Fine* stated that:

> Obviousness is tested by "what the combined teaching of the references would have suggested to those of ordinary skill in the art." *In re Keller*, 642 F.2d 413, 425, 208 USPQ 871, 878 (CCPA 1981)). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." *ACS Hosp. Sys.*, 732 F.2d at 1577, 221 USPQ at 933. And "teachings of references can be combined *only* if there is some suggestion or incentive to do so."

Id. (emphasis in original).

The M.P.E.P. adopts this line of reasoning, stating that:

> "In order for the Examiner to establish a *prima facie* case of obviousness, three base criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and

not based on Appellant s disclosure. *In re Vaeck* , 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir. 1991))". *M.P.E.P.* 2142

The test for obviousness under § 103 must take into consideration the invention as a whole; that is, one must consider the particular problem solved by the combination of elements that define the invention. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985). The Examiner must, as one of the inquiries pertinent to any obviousness inquiry under 35 U.S.C. § 103, recognize and consider not only the similarities but also the critical differences between the claimed invention and the prior art. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990), *reh'g denied*, 1990 U.S. App. LEXIS 19971 (Fed. Cir. 1990). Finally, the Examiner must avoid hindsight. *Id.*

Anticipation via a single prior art reference requires the disclosure in the reference of each element of the claim under consideration. *In re Dillon* 919 F.2d 688, 16 USPQ2d 1897, 1908 (Fed. Cir. 1990) (en banc), cert. denied, 500 U.S. 904 (1991).

2) Discussion of the Rejection of the Claims Under 35 U.S.C. § 103(a) as being unpatentable over Behr et al. in view of Hornbuckle and Ahrens et al.

The Examiner rejected claims 25-30 under 35 USC § 103(a) as being unpatentable over Behr et al. in view of Hornbuckle and Ahrens et al.

Claims 25-30 include encrypting the navigation data. The Examiner admits that "Behr et al does not teach encryption," and relies on Hornbuckle to disclose using encryption techniques in the distribution of software. However, there is no motivation to combine the references of Hornbuckle and Behr et al. and the rejection should be withdrawn.

Behr et al. describes a memory constrained system remote or mobile unit that does not contain detailed maps. It addresses the problem of providing more detail from a base station for a single route. Since the single route is of interest only to one user, it has no value to other users, and there is no need for encryption as provided for in all of the currently pending claims. All of

the discussion in Behr et al. of downloading up-to-date information is in the context of allowing a "mobile unit to operate with limited or no database storage..." Col. 22, lines 23-24. Further, information is downloaded to the mobile unit "for those portions of the route which are not adequately covered by maps available on-board the remote unit." Col. 21, line 67 to Col. 22, line 2.

The Office Action indicates that Hornbuckle provides motivation for securing transmitted software, citing "Behr et al's desire for sending software only to paying customers were accomplished without pirating/hacking by unauthorized, non-paying customers." No such desire is gleaned from Behr et al. As indicated above, Behr et al. transmit information related to selected routes, which is of interest only to the person seeking to follow the route. The Examiner suggests that Behr et al. disclose such a desire because Behr et al. discuss some of the problems associated with floppy disk distribution of software and map updates. The exact language cited by the Examiner:

> Another problem with autonomous route guidance systems is maintenance and currency of the database. As new streets are built, or as old streets are reconfigured, as businesses and other points of interest open and close, the database on CD-ROM or other media becomes out of date. In addition, when a database is compiled, it may include errors which are then replicated in the many copies provided to users. These errors may require correction in the user copies by replacing those database copies. Moreover, incorrect or outdated information in the database can lead to errors when calculating routes. When an out-of-date database does not include information that a particular roadway is closed, the system may be unable to calculate an alternate route.
>
> Autonomous route guidance system providers may improve the accuracy of the system by providing occasional database updates to users. However, distribution of the database, in a medium such as CD-ROM or floppy disk, to remotely located mobile users may be difficult. In addition, the media themselves are expensive since they may generally be used only a single time.

Col. 2, lines 4-24. As can be seen, Behr et al. recognize problems with costs and delays in such a method of updating databases. However, there is neither a suggestion to encrypt the information nor recognition of the problem discussed by Applicant, that an authorized update

could be applied to an unauthorized device. Because such limited information is being transmitted by the system of Behr et al., only information around a single route, there is no need for encryption. Hence, there is no motivation to combine Behr et al. with Hornbuckle, and the rejection should be withdrawn.

Ahrens et al. has been cited as stating that GPS updating methods can also be used for other types of software. It is not cited as providing a motivation to combine Behr et al. and Hornbuckle. While Ahrens et al. may indicate that GPS updating methods can also be used for other types of software, this does not strengthen the motivation to combine Hornbuckle and Behr et al. As indicted above, there is absolutely no need in Behr et al. for any type of encryption. The mere fact that GPS and software updates may be similar does not infer such a need.

Claims 25-30 also include "storing a unique software key within a GPS unit." Even if the references are combined, they do not suggest or teach this element of the claimed invention. By storing the unique software key in the GPS unit, the GPS unit is thus able to include it in a request for data to a software supplier as claimed. In contrast, Hornbuckle indicates that a key is stored in a remote control module 18, which decodes software and sends it to the target computer for execution. This portion of the method claimed is also not possible in Hornbuckle, since as the office action admits, it is the host in Hornbuckle that sends it to the module 18. It is simply not possible using the teaching of Hornbuckle to get the key to the target computer, nor for the target computer to then send it with a request for data. The Office Action indicates that it would have been obvious to one of ordinary skill at the time of the invention to have alternatively provided the host with a copy of the client key as part of the initial request, so that both parties have copies of the same key, consistent with the symmetric encryption approach. Since this is not possible in Hornbuckle, the assertion is respectfully traversed.

The Examiner also states that "Behr et al does not appear to specify example(s) where/how the unitID is stored with the device." Ahrens et al. is cited as providing hardware identification. While Ahrens et al. describe a media ID, the media ID is fundamentally different

from the unique software key described by Applicant. Applicant describes a unique software key that is used to encrypt data, so that only the proper device containing that key may run the downloaded software. In contrast, the system described by Ahrens et al. "reads the media ID and verify that it corresponds to this customer." Col. 20, lines 24-25. The data transferred is not encrypted, and the ID is certainly not used to do any encrypting. The unique software key and the media ID perform different functions and are of a substantially different character because of this. Thus, Ahrens et al. do not teach this limitation of the current invention.

The claims also include the "request including payment authorization information." The combination of the references also does not disclose this limitation. The phrase "payment authorization information" goes beyond "billing and audit information." The later describes where to send a bill. Payment of the bill is an entirely separate act. The bill can still be disputed and not paid. Payment authorization information is defined in the application as an actual method of payment, such as credit card information or means of electronic payment as indicated on page 8, lines 3-10. It is not merely billing and audit information as described in Behr et al. at col. 14, line 3. The Office Action indicates that the request for updated navigation information in Behr et al. inherently includes payment authorization information. Applicant respectfully disagrees because the Office Action has not established a *prima facie* case of inherency.

As recited in MPEP § 2112, "In relying upon the theory of inherency, the examiner must provide basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art," citing Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original). The Office Action appears to indicate that billing and audit information as well as information identifying the subscriber inherently includes payment authorization. Thus, the Office Action does not even assert that the allegedly inherent characteristic is necessary, let alone provide a basis in fact and/or technical reasoning. Applicant respectfully submits that payment authorization does not necessarily flow from billing information, because billing information

may only indicate where to send a bill. It does not inherently authorize payment. Since payment authorization does not necessarily flow from billing information, it is not an inherent characteristic, and the rejection should be withdrawn.

Applicant believes that the claims are in condition for allowance. There is no motivation to combine the cited references with Behr et al., and even if they were combined the combination fails to teach each element of the claimed invention. Applicant respectfully requests the withdrawal of all rejections to claims 25-30.

9. SUMMARY

Applicant believes the claims are in condition for allowance and requests withdrawal of the rejections to claims 25-30. Reversal of the Examiner's rejections of claims 25-30 in this appeal is respectfully requested.

Respectfully submitted,
KELLY E. DILLARD ET AL.
By their Representatives,
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Attorneys for Intel Corporation
P.O. Box 2938
Minneapolis, Minnesota 55402

Date August 10, 2004 By Monique M. Perdok Shonka
Monique Perdok Shonka
Reg. No. 42,989

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 10th day of August, 2004.

Dawn M. Poole
Name

Dawn M. Poole
Signature

APPENDIX I

The Claims on Appeal

1-24. (Canceled)

25. (Previously Presented) A method for providing navigation data to global positioning (GPS) units said method comprising the steps of:

storing a unique software key within a GPS unit;

forwarding a request from one of said GPS units for navigation data to a software supplier, said request including payment authorization information and a key code associated with the unique software key;

encrypting the navigation data by the supplier in response to said request using the included key code, said encrypted navigation data including a decryption program;

transmitting to the GPS unit having the stored unique software key, said encrypted navigation data including said decryption program which only allows software to be unloaded into a GPS unit having the unique software key;

decrypting said transmitted encrypted navigation data and decryption program at the one GPS unit according to the unique software key; and

replacing prior navigation data at the one GPS unit with the decrypted navigation data from the supplier.

26. (Previously Presented) The method in accordance with claim 25 wherein said step of encrypting the navigation data includes using cyclic redundancy coding.

27. (Previously Presented) The method in accordance with claim 26 wherein said step of encrypting the navigation data uses the GPS unit software key as a seed.

28. (Previously Presented) The method in accordance with claim 26 wherein the encrypted navigation data transmitted by the supplier includes a footer tag that includes the GPS unit software key.

29. (Previously Presented) The method of claim 28 wherein said step of decrypting said transmitted navigation data comprises reading the GPS unit software key from the footer tag and comparing the software key in the footer tag with the software key of the GPS unit.

30. (Previously Presented) A global positioning (GPS) unit for receiving updated navigation data from a system, the GPS unit comprising:

a processor;

a storage device coupled to the processor and storing a GPS unit unique software key;

a communication component coupled to the processor for connecting to a server over a network; and

a user interface coupled to the processor for requesting navigation data from the server, the request includes payment authorization information and a key code associated with the unique software key, wherein the communication component receives navigation data from the server that was encrypted by the server based on the request and the processor decrypts the encrypted navigation data as a function of the unique software key.